Havells India
ISMS Scope and Objectives

Version 1.2

Document Control

S No	Type of Information	Document Data
1.	Document Title	Havells India ISMS Scope and Objectives
2.	Document Code	HISMSSO
3.	Date of Release	20th Feb 2023
4.	Document Superseded	1.1
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Document Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

Sr. No.	Approver	Approver Designation	Nominee Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.1	26th Feb 2022	Updated scope statement	27th Feb 2022
1.2	20th Feb 2023	Updated IS objectives as per finding reference (2176951-202203-N1) of stage-2 assessment report	20th Feb 2023

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose 4

2. Introduction 4

2.1. Company profile 4

2.2. Havells’ approach to information security management 4

3. Information Security Management System Scope 5

3.1. Scope Statement 5

3.2. Applicability of Scope at Havells 5

4. Information Security Management System Objectives 6

1. Purpose

This document entails the details of the scope and objectives of Information Security Management System (ISMS) defined for Havells India (referred to as Havells/Company).

2. Introduction

2.1. Company profile

Havells India Limited is a leading Fast-Moving Electrical Goods (FMEG) company and a major power distribution equipment manufacturer with a strong global presence. Havells India Limited recognises the criticality and need of its business and understands the importance of availability of its critical business processes and services that support the key products and services. It also pays attention to the need for adequate information security measures to be in place.

2.2. Havells' approach to information security management

People, process, and technology are critical to the company for the conduct of its activities. By developing, documenting, implementing, and maintaining an Information Security Management System (ISMS) based on the ISO 27001 standard, Havells will have greater confidence in its personnel and the information security framework, and offer better assurance to its customers.

An ISO 27001 certification makes a public statement of capability, whilst permitting the organization to maintain the confidentiality, integrity, and availability of its information and assets. An ISO 27001 certification also provides competitive advantage to Havells in the marketplace, as it puts Havells in the league of those organizations that comply with a globally accepted and respected information security standard.

Havells has adopted a structured phased approach to information security risk management. The approach can be broadly classified into three distinct phases:

a) Preparation of ISMS documentation (inclusive of all relevant records) in order to apply for certification;

b) Implementation of the ISMS; and

c) Certification process

Havells' IT Team and respective or concerned business/functional team shall provide inputs for scope definitions.

The following is the input for scope definition for Havells India:

Department	Inputs for scope definition
Information Technology	The IT department shall be responsible for the following activities, but not limited to: a) Devising and implementing the information security policies for the organization.

Department	Inputs for scope definition
	b) Managing and maintaining the IT infrastructure of Havells; c) Maintaining applications that are being used by various business functions; d) Vendor management for different IT support services for maximizing the efficiency of IT operations and maintenance of applications; and e) Conducting assessment of Havells' security posture and providing inputs to the management on the key improvement areas.

Table 1: Input for scope definition

3. Information security management system scope

3.1. Scope statement

The ISMS at Havells India Ltd. applies to its IT Department and it's Interfaces with functions of HR, Administration, Sales, Procurement Management, Finance & Accounts, Quality Assurance, Production & Inventory from its corporate office at Noida.

3.2. Applicability of scope at Havells

The information security management system scope encompasses the following enablers:

Scope Enablers	Description
Location	The corporate office of Havells India and the data center at Noida and Bangalore are covered under the scope for this ISMS
Functions	IT department
Personnel	All employees/third party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

Non-IT Assets (Hardware/Equipment)	Non-Information assets include, but not restricted to, the following
	a) Air-conditioning systems;
	b) Power generators;

Information Assets (Hardware and Software)	Information assets include, but not restricted to, the following: a) Project and process related documents; b) Accounting information (bills, invoices); c) Electronic documents maintained; d) Master Service Agreements (MSAs); e) Operational policies and procedures in electronic format; f) Key applications (SAP ECC, SAP GRC, etc.) and software's (Network Management Systems, IDS/IPS, Firewall, Network, and communication links, etc.); g) Servers; h) Workstations (desktops, laptops) and IT accessories (keyboard, mouse, charger, etc.); i) Backup devices; and

Scope Enablers	Description
	j) Network devices and cables, etc.

Table 2: Applicability of scope

4. Information Security Management System Objectives

Information security objectives is to implement strategic goals of the organization in line with Organizational business objectives. This objective will supplement respective functional or business Policies, Procedures (SOPs) and DOAs to achieve overall organizations' s business objectives. The objective of information security management system at Havells is developed in accordance with ISMS objectives as per ISO 27001-2013.

Information Security Objectives focuses on Confidentiality, Integrity and Availability of the information to facilitate business requirements considering the following at relevant Functional and Business levels.

I. To protect the organization's network, systems, applications and data from unauthorized access, malware and hacking/ Ransomware attempts by implementing appropriate security measures, such as Firewalls, Email Security, VAPT, Web Application . Firewalls, Next-gen Antivirus, Secure Web Gateways, DLP

II. Protection of critical information assets by implementing access controls, role based access controls and encryption technologies

III. To maintain the integrity of information by ensuring that it is not modified, deleted, or destroyed without authorization

IV. To improve the availability of information and information systems by implementing redundancy, backup, and recovery measures

V. To enhance the security awareness and training of users by providing regular security awareness training sessions and communications

VI. To comply with relevant legal, regulatory, and contractual requirements by implementing appropriate security controls

VII. To continuously improve the effectiveness of the information security management system by conducting regular audits and reviews

VIII. To have an effective Business Continuity Plan in place that is regularly tested, updated and communicated to all stakeholders

IX. Third-party vendors and partners comply with the organization's information security policies and standards, and effectively manage the risk of sharing information with them

X. Changes to the information system are managed effectively, minimizing the risk of errors, outages and unauthorized access

XI. To regularly review and assess information security risks and threats, and implement risk mitigation measures to minimize the potential impact on the organization

While defining KPI / KRA, respective functions should consider following elements to ensure their operating effectiveness-

a. Ensure consistency in processes
b. KPI / KRA should be measurable wherever possible
c. Risk Identification, Assessment, Rating, Response and Treatment